Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/IL04/000781

International filing date: 29 August 2004 (29.08.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/535,507
Filing date: 12 January 2004 (12.01.2004)

Date of receipt at the International Bureau: 23 November 2004 (23.11.2004)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/IL2004/000781
16 NOV 2004

PA 1245136

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

November 05, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: *60/535,507*
FILING DATE: *January 12, 2004*

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

M. Sias

M. SIAS
Certifying Officer

Please type a plus sign (+) inside this box → +

Docket Number: 3140/1

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

INVENTOR(S)/APPLICANT(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
REUVEN	ZEITAK	REHOVOT, ISRAEL

□ Additional inventors are being named on page 2 attached hereto

TITLE OF THE INVENTION (280 characters max)

A POLICER AND METHOD FOR RESOURCE BUNDLING

CORRESPONDENCE ADDRESS

Direct all correspondence to:

□ Customer Number ______ → Place Customer Number Bar Code Label here

OR

☒ Firm or Individual Name	Mark M. Friedman				
Address	c/o DISCOVERY DISCOVERY				
Address	9003 FLORIN WAY				
City	UPPER MARLBORO	State	MD	ZIP	20772
Country	US	Telephone	301-952-1011	Fax	301-952-9023

ENCLOSED APPLICATION PARTS (check all that apply)

☒ Specification	Number of Pages 12		
☒ Drawing(s)	Number of Sheets 6	☒ Other (specify)	ASSIGNMENT

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)

		FILING FEE AMOUNT
□ A check or money order is enclosed to cover the filing fees		
☒ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number:	06-2140	$80 + $40

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

□ Yes, the name of the U.S. Government agency and the Government contract number are: ______

Respectfully submitted,

SIGNATURE ______ DATE 8 JAN 04

TYPED or PRINTED NAME Mark M. Friedman

REGISTRATION NO. (if appropriate) 33,883

TELEPHONE (703) 415-1581

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, DC 20231

Company Confidential
Native Networks Technologies, Ltd.

Invention Name	A Policer and Method for Resource Bundling
Patent Disclosure Number	NNW-003
Lawyer Reference Number	
Inventor(s)	Reuven Zeitak
Assignee	Native Networks Technologies, Ltd.
Date	

Abstract

A policer and method for resource bundling are disclosed. The invention disclosed serves a plurality of classes of service (CoS) of a plurality of different data flows, and shares the available bandwidth among the data flows in a prioritized manner. Accordingly it allows a single user to aggregate multiple CoS, thus enabling the user to utilize the entire bandwidth paid for.

Technical Field

The present invention relates generally to communication networks, and more particularly to methods for policing data traffic in communication networks.

Background of the Invention

Today's communication networks are more diverse and bandwidth-intensive than ever before. High bandwidth communication networks are frequently required when a user needs to transmit a digital data stream. Often the data stream includes data of different priority, ranging from high priority data, e.g., voice communications, which cannot tolerate significant delays, to low priority data, e.g., file transfers.

Access to communication networks is typically provided by a service provider who maintains equipment at nodes on the network. Generally, service providers supply access to the network for multiple users. A user can access the network with multiple data streams. In order to secure sufficient bandwidth, users often contract for discrete channels, each channel capable of handling the greatest expected bandwidth requirement of a respective data stream. Often, these channels utilize only a small fraction of the maximum allocated bandwidth. As a result, a user either pays for potential bandwidth and using only a fraction thereof, or a user takes advantage and uses bandwidth at rates beyond what was actually paid for. In order to enable users to pay only for utilized bandwidth, service providers limit the transmission rate. Means for limiting and controlling the traffic are even more essentially in a network employing a non-deterministic access protocol, such as an Ethernet network or a metro Ethernet network (MEN).

Typically, service providers offer a user a range of services that are differentiated based on some performance characteristics, such as delays and packet losses. Specifically, a user purchases a service package that assures the user a certain level of service level usually referred to as quality of service (QoS). A service package is determined by a bandwidth profile and a class of service (CoS). The bandwidth profile is a set of traffic parameters that governs the expected arrival pattern of user traffic and provides a deterministic upper bound, or an envelope to the expected volume of traffic. The bandwidth traffic parameters are: committed information rate (CIR), committed burst size (CBS), excess information rate (EIR), and excess burst size (EBS). The CoS defines the treatment inside the provider network, i.e., the level of delay requirement. For example, a packet with a high priority level CoS may be forwarded at the highest priority to assure minimum processing delay.

The traffic management is performed by the policing function implemented in a device (hereinafter the "policer"), of a network access node. The policer enforces the rate on each incoming data flow or a set of data flows as designated in the service package and as characterized by the bandwidth. The first step in rate enforcement is to determine the level of conformance of the incoming data flow. The level of conformance is typically expressed as one of three colors: green, yellow, or red, where green packets are transmitted at a rate equal to the CBS, yellow packets are transmitted at a rate equal to the EBS, and red packets are not transmitted.

One of the algorithms to compute the level of conformance of incoming data flows is a token bucket rate algorithm (TBRA). For each incoming flow the TBRA determines whether to accept or reject an incoming flow. A flow is accepted if its length is less than the bucket contents; otherwise the flow is rejected. The bucket contents at time t_j, is calculated using the equation:

$$B_j = MIN[L, B_{j-1} + R \times (t_j - t_{j-1})]; \qquad (1)$$

where, B_j is the bucket content at time t_j, L is the bucket length (i.e., the burst size), and R is the rate. The parameters (L, R) can be replaced by the parameters (CBS, CIR) or (EBS, EIR) and therefore the TBRA can be used to determine the level of conformance for "green packefs" and "yellow packets".

It should be noted that different algorithms based on the principle described in the TBRA may be found in prior art discussions. For example, three color marker, leaky bucket, adaptive leaky bucket, one bucket two colors, just to name a few.

Currently, policers are not designed to share the available bandwidth according to the CoS. Specifically, the bandwidth can be shared either among an aggregation of data flows with different CoS, or set of data flows with the same CoS. In the former case, data flow is served on a basis of "first comes first served", where in the latter case, for each CoS a constant rate, as defined by CIR, is assured. However, in both cases a policer neither can serve more than one data flow and more than one CoS, nor share the bandwidth efficiently between different levels of CoS.

Therefore, in the view of the limitations introduced in the prior art, it would be advantageous to provide a policer that handles multiple CoS and data flows. It would be further advantageous if such a policer shares the bandwidth allocated to a single user in a prioritized manner.

Brief Description of the Drawings

Figure 1 – is an exemplary diagram of a policing unit for the purpose of illustrating the principles of the present invention

Figure 2 – is a time diagram illustrating the operation of the disclosed policer

Figure 3 – is a time diagram illustrating one of the capabilities of the disclosed policer

Figure 4 - is an exemplary embodiment of an algorithm used for policing data flows

Figure 5 – is a non-limiting block diagram of the disclosed policer

Figure 6 - is an exemplary for another embodiment for policing data flows

Detailed Description of the Invention

The present invention provides a method and a policer for resource bundling in networking systems. The invention disclosed serves a plurality of classes of service (CoS) of a plurality of different data flows and shares the available bandwidth among the data flows in a prioritized manner. Accordingly, it allows a single user to aggregate multiple CoS, and hence enabling a low priority CoS to consume bandwidth when a high priority CoS is idle. This ensures that a user utilizes the entire bandwidth paid for, namely the bandwidth is not shared among other users when the high priority CoS data flow of a user is idle, i.e., paid for bandwidth is first used for lower priority packets of the paying user rather than being utilized by high priority packets of another user not paying for the additional bandwidth that may be needed.

Reference is now made to Fig. 1 where an exemplary diagram of a policing unit (PU) 100 for the purpose of illustrating the principles of the present invention, is shown. PU 100 includes 'n' policers 110-1 through 110-n connected in a cascade connection. Policer 110 is parameterized by the pairs (CIR, CBS) or (EIR, EBS). For each policer 110 a coloring unit (CU) 120 is attached. Each CU 120 marks the packets with a different color as preconfigured by the service provider. For example, data packets passing through policer 110-1 are considered to be colored in green, while packets passing through policer 110-2 are considered to be colored in yellow. Policer 110 includes a plurality of thresholds, where each threshold defines the allowed burst size for a CoS priority level. For each received data packet, policer 110 performs a conformance check to determine whether to accept or reject an incoming packet. The decision is based on a preconfigured threshold as well as the available bandwidth, as described in greater detail below. As can be seen in Fig. 1, policer 110-1 can accept or reject packets with a high priority CoS or a low priority CoS.. High priority CoS packets have priority over low priority CoS packets regardless of the amount of available bandwidth. Packets accepted by policer 110-1 are colored in green, while packets rejected by policer 110-1 are forwarded to policer 110-2, which handles only lower priority CoS packets.

Policer 110 includes various configurable parameters. The configurable parameters include, but are not limited to, the CoS priority levels to be handled by the policer, the thresholds, the colors to mark accepted packets, CIR, CBS, EIR, EBS, and others. This allows a service provider to define and offer a plurality of different service packages for different users. For example, a client may purchase a service package of 10 Mbps of CIR and 4KB of CBS for high priority CoS, as well as 5 Mbps of EIR for low priority CoS. The service package may include the rule that when flows of the high priory CoS are inactive, flows of the low priority CoS may also use the CIR with a burst less than 2KB. For such service package, the service provider configures the low priority threshold to the value of 2KB and the high priority thresholds to the value of 6 KB (i.e., the 4 KB requested as a minimum for the high priority CoS plus the 2KB for the low priority CoS).

Reference is now made to Fig. 2 where a time diagram illustrating the operation of policer 110 in accordance with the disclosed invention, is shown. Fig. 2 shows the behavior of policer 110 that includes two threshold levels 210 and 220 respectively.

While the operation of the policer herein is discussed for only two thresholds, this is performed for exemplary purposes only, and multiple threshold levels may be used as may be necessary for the particular application. Thresholds 210 and 220 define the permitted burst size for a low priority CoS and a high priority CoS respectively. At time t_0, policer 110 has enough bandwidth, i.e., credit to accept either a high priority packet (i.e., a packet with a high priority CoS) or a low priority packet as along as the length of the incoming packet is smaller than the CBS. A packet's length is tolerated between a maximum length and a minimum length as defined by the protocol type. At time t_1, a low level priority packet 230-1 with length l_1 is received. Since, the length l_1 is smaller than the burst size of threshold 210 (i.e., $l_1 < TH_L$) packet 230-1 is accepted by policer 110-1. As a result, the credit's value is set to be the value of the current credit (C_0) minus the length l_1. At time t_2, a high priority packet 230-2 with length l_2 is received. As the value of the current credit (C_2) minus the length of packet 230-2 does not exceed threshold 220 (i.e., $C_2 - l_2 < TH_h$), packet 230-2 is accepted. As a result, the credit's value is set to the value of the current credit (C_2) minus the length l_2. At time t_3, a high level packet with length l_3 is received. The credit value at time t_3 (C_3) minus the length of packet 230-3 (l_3) exceeds threshold 220 (i.e., $C_3 - l_3 > TH_h$) and therefore packet 230-3 is rejected. The credit value increases as a function of the rate, i.e., CIR or EIR. Specifically, the credit value at time t_i (C_j) can be calculated using the equation:

$$C_j = \min\lfloor CBS, C_j + CIR \times (t_j - t_{j-1}) \rfloor. \qquad (2)$$

The credit, the length of a packet, and the burst size are typically measured in bytes.

Reference is now made to Fig. 3A where a time diagram demonstrating one of the capabilities of policer 110 to protect high priority CoS data flows against flooding from low priority CoS data flows in accordance with the disclosed invention, is shown. At time t_2 a low priority packet 330-1 with length l_1 is received. The credit value at time t_2 (C_2) minus the length of packet 330-1 (l_1) exceeds the low level threshold 310 (i.e., $C_2 - l_1 > TH_L$), and for that reason packet 330-1 is rejected. Subsequently, a high priority packet 330-2, having length l_2, is received. Due to the fact that the value of the current credit (C_2) minus the length l_2 does not exceed the high level threshold 320 (i.e., $C_2 - l_2 < TH_h$) packet 330-2 is accepted. As can be seen in Fig. 3B, accepting packet 330-1 would have caused the rejection of packet 330-2, since there is not enough bandwidth to serve both packets.

Referring now to Fig. 3C where another example for the operation of policer 110 is provided. From time t_0 to time t_4 four consecutive data packets 310-1 through 310-4 all belong to a low priority data flow are arrived. The lengths of data packets 310-1, 310-2, 310-3, and 310-4 are l_1, l_2, l_3, and l_4 respectively. At time t_1, packet 310-1 is accepted, since the credit value at time t_1 (C_1) minus the length of packet 330-1 (l_1) does not exceed the low level threshold 310 (i.e., $C_1 - l_1 > TH_L$). At time t_2, packet 310-2 is accepted, although the credit value at time t_2 (C_2) minus the length of packet 330-2 (l_2) exceeds the low level threshold 310 (i.e., $C_2 - l_2 < TH_L$). This is done in order to allow a user to consume the entire bandwidth paid for, when high priority flow is not transmitted, i.e., no high priority packets are received. The same is true for packet 330-3 arrives at time t_3. At time t_4, packet 310-4 is rejected to leave enough bandwidth to high priority packet 310-5. This is done in order to eliminate the acceptance of the low priority flows in favor of high priority flows. At time t_5 packet 310-5 is accepted, since the credit value at time t_5 (C_5) minus the length of packet 330-5 (l_5) does not exceed the high level threshold 320 (i.e., $C_5 - l_5 > TH_h$).

As can be understood from the exemplary cases described above, the use of multiple thresholds allows the sharing of bandwidth allocated to a single user in a prioritized manner. Furthermore, as policer 110 is allocated per user, a single user may aggregate multiple CoS and thus allow for low priority data flows to consume bandwidth allocated for high priority data flows, when such high priority flows are not transmitted, but that bandwidth was paid for anyway. This is in contrast with prior art solutions where unused bandwidth allocated for high priority flows is shared among other users. That is, policer 110 is designed to provide means for resource bundling.

Reference is now made to Fig. 4 where an exemplary embodiment of an algorithm 400 used for policing data flows in accordance with this invention, is shown. At step S410, a packet 'j' with a length l_j is received. At step S420, the incoming packet is analyzed to determine the CoS priority level of the packet. The CoS's priority level is designated in the packet header. At step S430, for packet 'j' arrives at time t_j, a tentative Credit value ("B") is calculated. The tentative credit value determines the remaining credit after accepting an incoming packet. The tentative credit value is calculated using the following equation:

$$B = C_j - l_j; \qquad (3)$$

where, C_j is the available credit at time t_j and l_j is the length of an incoming packet 'j'. The value of C_j may be calculated using equation (2). At step S440 the tentative credit value is compared against the CoS threshold (TH_{CoS}) corresponding to the CoS priority level of the incoming packet. If the value of the tentative credit value is lower than the threshold value (i.e., $B < TH_{CoS}$), then, at step S450, the packet is accepted; otherwise, at step S470, the packet is rejected. As a result of accepting the packet, at step S460 the credit C_j is set to the value of the tentative credit value. A rejected packet can be forwarded to another policer of a lower level, or alternatively it may be dropped.

The method described herein is capable of handling multiple data flows. Data flows are data packets, or service frames that have been analyzed for the purpose of determining the process flow to which they belong, how the packets should be processed, where the packet should be routed, and so on. For example, a process flow may be a series of packets all belonging to the signaling of a file transfer protocol (FTP).

Reference is now made to Fig. 5 where a non-limiting block diagram of policer 110 is shown. Policer 110 comprises of an input port 505 and an output port 575. Policer 110 further includes a receiver 510, a transmitter 520, a determination unit (DU) 530, a computing unit (CU) 540, and a comparator 550. Input port 505 and output port 575 may be, but are not limited to, 10Mbp, 100Mbps, 1Gbps, and 10Gps Ethernet ports. Input and output ports are both coupled to a common communication link. Receiver 510 is coupled to input port 505 and to DU 530, that is connected to CU 540. CU 550 is connected to comparator 550 that is further coupled to transmitter 520.

Receiver 510 receives the incoming data packets being transported over the common communication link. Upon reception of a data packet, receiver 510 provides the information of the header part of this data packet to DU 530. DU 530 determines, from the received header information, the CoS priority level and the length of the incoming packet. DU 530 provides comparator 550 with the CoS priority level information and CU 540 with the packet's length. CU 540 computes the tentative credit value (B), for example, according to equation (3), and provides comparator 550 with the result. Comparator 550 executes a conformance check according to the predefined threshold and the CoS priority level of the packet. Comparator 550 determines if the calculated tentative credit value (B) exceeds the predefined threshold, and if it is the packet is rejected; otherwise, the packet is accepted. In the event that comparator 550 declares the received packet as accepted, the packet may be transmitted on the communication link. As a result, comparator 550 forwards a permission signal to the transmitter 520 that subsequently transmits the packet on the communication link. If the received packet is rejected, then the packet is not transmitted on the communication link.

It should be appreciated by a person skilled in the art that the components of policer 110 described herein may be hardware components, firmware components, software components, or combination thereof.

In an embodiment of this invention policer 110 is opted to be included in a metro Ethernet network (MEN) on the user-network interface (UNI) using a standard 10Mbp, 100Mbps, 1Gbps, 10Gps Ethernet interface. In the MENs, policer 110 may carry out all the activities related to Ethernet traffic management as described in greater detail above.

Reference is now made to Fig. 6 where another embodiment used for policing data flows in accordance with this invention is provided. Fig. 6 shows a set of 'n' counters 610-1 through 610-n, each of counters 610 serves a different priority level of CoS. A counter 610-i counts at a rate proportional to the committed rate until its threshold is reached. Once the threshold is reached the next counter 610-i+1 starts to accumulate credit. Specifically, when a packet arrives, its length is compared to the amount of available credit in counters 610 and the packet is deemed conforming or non conforming based on a preprogrammed rule. As non-limiting example, a packet with a CoS priority level 'j' is accepted if the following rule is obeyed:

$$l > CC_j + CC_{j+1} + \ldots + CC_n.$$

Wherein, l is the length of the packet amd CC_i is the is the amount of credit in the counter 610-i. The CoS priority levels of counter 610-1 through 610-n are CoS_1 through CoS_N respectively, where CoS_1 is the highest priority and CoS_N is the lowest priority.

After which, the counters are depleted, starting with CC_N until a total of length 'l' credit has been removed.

What We Seek to Protect

1. A method for sharing data allocated to a single user in a prioritized manner
2. A computer executable code for sharing data allocated to a single user in a prioritized manner
3. A policer capable of resource bundling

Exemplary and Non-Limiting Claims

1. *A method for sharing data flow bandwidth allocated to a single user in a prioritized manner, wherein said method capable of handling a plurality of class of service (CoS) priority levels of a plurality of different data flows, said method comprises the steps of:*

   a) receiving a packet belongs to one of said data flows;

   b) determining said CoS priority level of said packet;

   c) calculating a tentative credit value;

   d) comparing said tentative credit value against a CoS threshold;

   e) accepting said packet if said tentative credit value is lower than said CoS threshold; and,

   f) rejecting said packet if said tentative credit value exceeds said CoS threshold.

2. The method of claim 1, wherein said tentative credit value determines the remaining available bandwidth upon accepting said packet.

3. The method of claim 1, wherein said CoS threshold defines the permitted burst size for said CoS priority level.

4. The method of claim 1, wherein said CoS threshold is a configurable value..

5. The method of claim 1, wherein the step of accepting said packet further comprises the steps of:

   a) setting the available credit to said tentative credit value;

   b) marking said packet with a color tag; and,

   c) transmitting said packet on a network.

6. The method of claim 5, wherein said network is at least one of: Ethernet network, metro Ethernet network (MEN).

7. *A computer executable code for sharing data flow bandwidth allocated to a single user in a prioritized manner, wherein said method capable of handling a plurality of class of service (CoS) priority levels of a plurality of different data flows, said code comprises the steps of:*

   a) receiving a packet belongs to one of said data flows;

b) determining said CoS priority level of said packet;

c) calculating a tentative credit value;

d) comparing said tentative credit value against a CoS threshold;

e) accepting said packet if said tentative credit value is lower than said CoS threshold; and,

f) rejecting said packet if said tentative credit value exceeds said CoS threshold.

8. The computer exactable code of claim 7, wherein said tentative credit value determines the remaining available bandwidth upon accepting said packet.

9. The computer exactable code of claim 7, wherein said CoS threshold defines the permitted burst size for said CoS priority level.

10. The computer exactable code of claim 7, wherein said CoS threshold is a configurable value.

11. The computer exactable code of claim 7, wherein the step of accepting said packet further comprises the steps of:

a) setting the available bandwidth to said tentative credit value;

b) marking said packet with a color tag; and,

c) transmitting said packet on a network.

12. The computer exactable code of claim 11, wherein said network is at least one of: Ethernet network, metro Ethernet network (MEN).

13. *A policer for resource bundling, wherein said policer is capable of serving a plurality of class of service (CoS) priority levels of a plurality of different data flows, said policer comprises at least:*

an input port coupled to a common communication link;

an output port coupled to said common communication link;

means for receiving data packets transmitted over said common communication link;

means for determining said CoS priority level and a length of each of said data packets;

means for computing a tentative credit value for each of said data packets;

means for comparing said tentative credit value against a CoS threshold for of each said data packets; and,

means for transmitting said data packets over said common communication link if accepting said data packets.

14 The policer of claim 13, wherein said network is at least one of: Ethernet network, metro Ethernet network (MEN).

15. The policer of claim 13, further comprises a plurality of CoS thresholds each of said CoS thresholds corresponding to said CoS priority level.

16. The policer of claim 15, wherein said CoS threshold defines the permitted burst size for a CoS priority level.

Figures

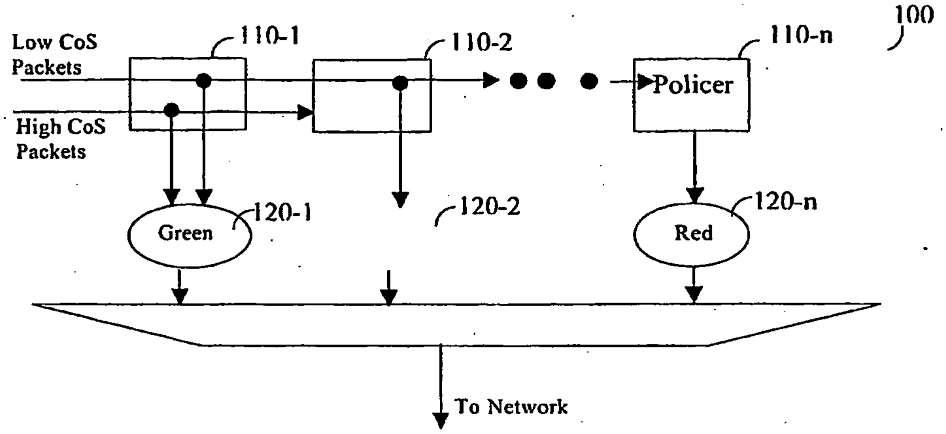

FIGURE 1

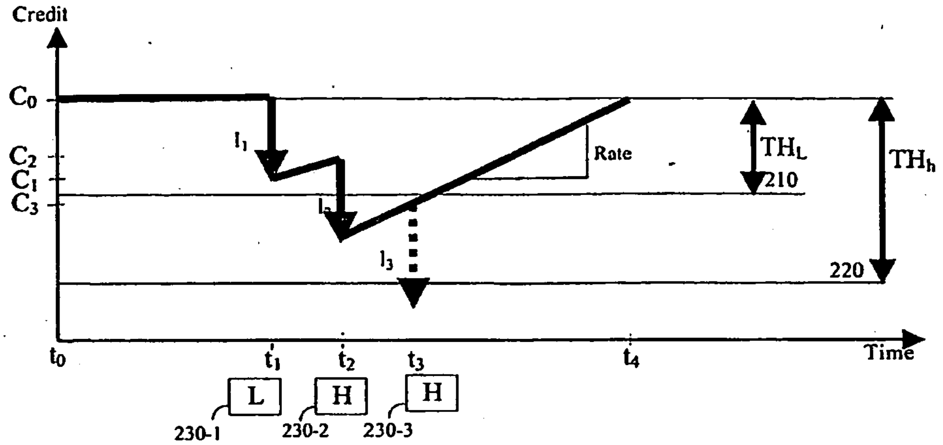

FIGURE 2

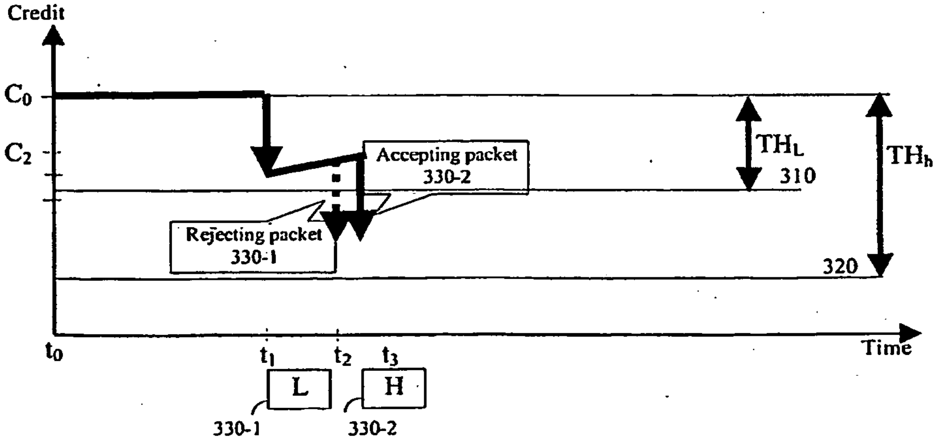

FIGURE 3A

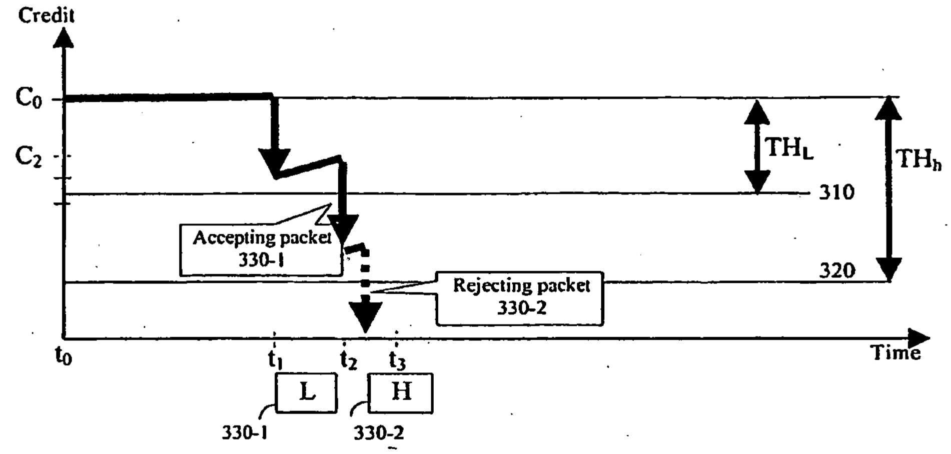

FIGURE 3B

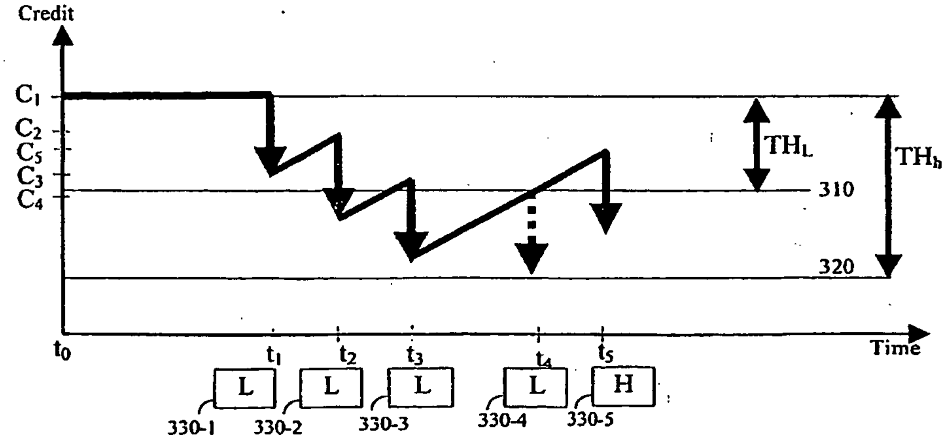

FIGURE 3C

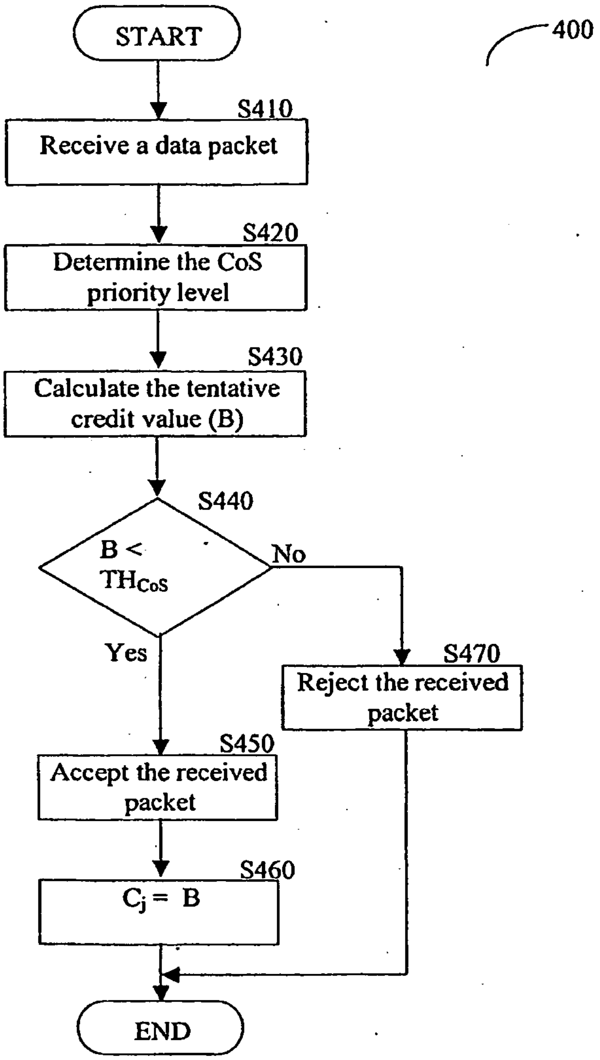
400
START
S410
Receive a data packet
S420
Determine the CoS priority level
S430
Calculate the tentative credit value (B)
S440
B < TH$_{CoS}$
No
Yes
S470
Reject the received packet
S450
Accept the received packet
S460
$C_j = B$
END

FIGURE 4

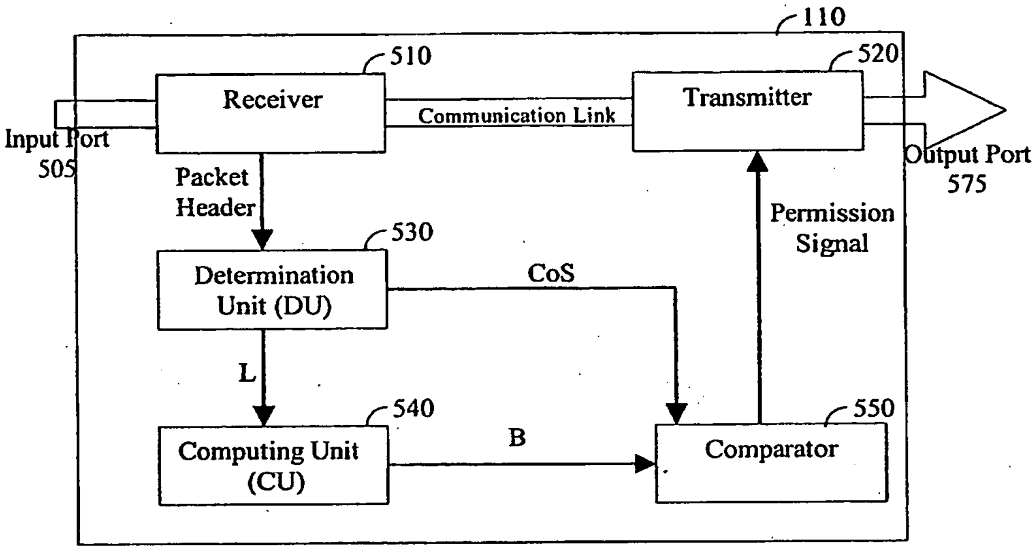
110
510
Receiver
Communication Link
520
Transmitter
Input Port
505
Output Port
575
Packet
Header
530
Determination
Unit (DU)
CoS
Permission
Signal
L
540
Computing Unit
(CU)
B
550
Comparator

FIGURE 5

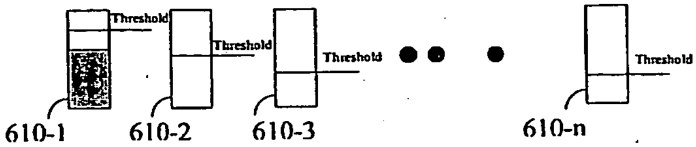
Threshold
Threshold
Threshold
Threshold
610-1
610-2
610-3
610-n

FIGURE 6

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING SUBMISSION OR TRANSMITTAL OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

FRIEDMAN, Mark
7 Jabotinsky St.
52520 Ramat Gan
ISRAËL

Date of mailing *(day/month/year)* 29 November 2004 (29.11.2004)	
Applicant's or agent's file reference 3140-2	**IMPORTANT NOTIFICATION**
International application No. PCT/IL04/000781	International filing date *(day/month/year)* 29 August 2004 (29.08.2004)
International publication date *(day/month/year)*	Priority date *(day/month/year)* 12 January 2004 (12.01.2004)
Applicant NATIVE NETWORKS TECHNOLOGIES, LTD. et al	

1. By means of this Form, which replaces any previously issued notification concerning submission or transmittal of priority documents, the applicant is hereby notified of the date of receipt by the International Bureau of the priority document(s) relating to all earlier application(s) whose priority is claimed. Unless otherwise indicated by the letters "NR", in the right-hand column or by an asterisk appearing next to a date of receipt, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).

2. *(If applicable)* The **letters "NR"** appearing in the right-hand column denote **a priority document which, on the date of mailing of this Form, had not yet been received by the International Bureau** under Rule 17.1(a) or (b). Where, under Rule 17.1(a), the priority document must be submitted by the applicant to the receiving Office or the International Bureau, but the applicant fails to submit the priority document within the applicable time limit under that Rule, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

3. *(If applicable)* **An asterisk (*)** appearing next to a date of receipt, in the right-hand column, denotes **a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b)** (the priority document was received after the time limit prescribed in Rule 17.1(a) or the request to prepare and transmit the priority document was submitted to the receiving Office after the applicable time limit under Rule 17.1(b)). Even though the priority document was not furnished in compliance with Rule 17.1(a) or (b), the International Bureau will nevertheless transmit a copy of the document to the designated Offices, for their consideration. In case such a copy is not accepted by the designated Office as the priority document, Rule 17.1(c) provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
12 January 2004 (12.01.2004)	60/535,507	US	23 November 2004 (23.11.2004)

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 740 14 35	Authorized officer Olaiz Alicia Facsimile No. +41 22 338 71 30 Telephone No. +41 22 338 9288